

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

VALERIE TORRES, et al.,
Plaintiffs,

v.

PRUDENTIAL FINANCIAL, INC.,
ACTIVEPROSPECT, INC., and
ASSURANCE IQ, LLC,
Defendants.

Case No. 22-cv-7465-CRB

**ORDER GRANTING CLASS
CERTIFICATION**

Lead Plaintiffs Valerie Torres and Rhonda Hyman bring this consumer privacy class action against Defendants Prudential Financial, Inc., ActiveProspect, Inc., and Assurance IQ, LLC. Plaintiffs allege that ActiveProspect intercepted and recorded without consent their real-time interactions with a form on Prudential's website in violation of the California Invasion of Privacy Act, and that Prudential and Assurance aided in this violation. Plaintiffs now move for certification of a class defined as follows:

All natural persons who, while in California, visited Prudential.com, provided personal information on Prudential's form to receive a quote for life insurance, and for whom a TrustedForm Certificate URL associated with that website visit was generated from November 23, 2021 to December 13, 2022.

Plaintiffs also move to appoint themselves as class representatives and Girard Sharp LLP as class counsel. Id. The Court finds the matter suitable for resolution without oral argument pursuant to Local Civil Rule 7-1(b) and **GRANTS** Plaintiffs' motion.¹

¹ After the parties finished briefing class certification, Defendants filed a motion for summary judgement. They ask the Court to resolve that motion before class certification. See MSJ (dkt. 93) at 2. But Plaintiffs' claims in this case are not so obviously "meritless" that it would be wasteful to certify a class at this time, so the Court resolves the motions in

I. BACKGROUND**A. Factual History**

The Court described the facts giving rise to this lawsuit in its order on Defendants' motion to dismiss, see MTD Order (dkt. 29), available at 2023 WL 3933073, and repeats here only those facts necessary to resolve the motion at hand.

During the class period, Prudential and its wholly owned subsidiary, Assurance, designed and operated a form on Prudential's website that individuals could fill out to obtain a life insurance quote. Am. Compl. (dkt. 18) ¶ 1; Opp. (dkt. 81) at 2. The form prompted users to enter information about their demographics, family situation, and medical history. Am. Compl. ¶¶ 45–46. Prudential and Assurance added ActiveProspect's TrustedForm script to the source code, enabling ActiveProspect to intercept and record users' real-time interactions with the form. Rafferty Dep. Tr. (dkt. 66-6) at 112:21–113:8.

TrustedForm functions as follows: When a user navigates to the first page of the form, TrustedForm issues a unique identifier—the “Certificate URL”—for that user and “initiate[s] a series of more than one hundred [] requests” to send data from the user's web browser to ActiveProspect's server. Id. at 105:24–106:7; Shafiq Rpt. (dkt. 66-3) ¶ 22.

TrustedForm allows ActiveProspect to collect information about users, including:

- User metadata, such as the user's public IP address. Shafiq Rpt. ¶¶ 23, 51; ActiveProspect Sept. 20, 2023 Blog Post (dkt. 81-19) at 2.
- The user's “real-time interactions” with the form, including keystrokes, mouse movements and clicks, and data inputs.² Shafiq Rpt. ¶¶ 16, 31–32, TrustedForm End Use License Agreement (dkt. 66-9) at 2.

ActiveProspect uses the data it collects to recreate a visual “session replay” (resembling a

the order it received them. Contra Cavanagh v. Humboldt County, No. C 97-4190 CRB, 1999 WL 96017, at *2 (N.D. Cal. Feb. 22, 1999).

² Prudential's form asked for—and TrustedForm therefore captured—the following information about the person seeking life insurance: gender; marital status; date of birth; height and weight; employment status; whether the person has children; and health and medical information, including whether the person has been treated for anxiety, depression, bipolar disorder, heart or circulatory disorders, cancer, respiratory disorders, chronic pain, and various other medical conditions. Shafiq Rpt. ¶ 39.

video recording) of the user’s real-time interaction with the form. Shafiq Rpt. ¶¶ 45, 48. It then issues a “TrustedForm Certificate” containing the collected information and session replay for each user that interacts with the form. *Id.* ¶¶ 45–47. Prudential and Assurance can access a particular user’s “TrustedForm Certificate” using the “Certificate URL” associated with that user. *Id.* ¶ 77; Rafferty Dep. Tr. at 105:24–06:18.

Between March 2022 and January 2023, Plaintiffs visited the form on Prudential’s website and entered the requested information to obtain a life insurance quote. Am. Compl. ¶¶ 65, 69. Prudential did not expressly disclose to Plaintiffs that a third party was recording their interactions with the form until Plaintiffs had completed the form and clicked “Get an instant quote.” *Id.* ¶ 74. Only then were Plaintiffs provided with a link to Prudential’s privacy policies and required to accept its terms to obtain a quote. *Id.* ¶¶ 45–46, 74–76. Plaintiffs assert that at the time they filled out the form, they were not aware of and did not consent to ActiveProspect’s interception and collection of their information, including keystrokes, mouse clicks, and data inputs. *Id.* ¶¶ 64, 68, 72; Hyman Dep. Tr. (dkt. 81-4) at 206:1–206:20; Hyman Decl. (dkt. 66-23) ¶ 4; Torres Decl. (dkt. 66-24) ¶ 4.

Plaintiffs allege that Defendants violated section 631(a) of CIPA, which makes liable anyone who “willfully and without the consent of all parties to the communication ... reads or attempts to read, or to learn the contents or meaning of any ... communication while the same is in transit over any wire, line, or cable, or is being sent from, or received at any place within [California] ... or who aids ... any person” with the same conduct. They now seek to certify a class under Federal Rule of Civil Procedure 23(b)(3).

II. STANDING

A. Legal Standard

Before considering Plaintiffs’ motion for class certification, the Court must determine whether Plaintiffs have standing under Article III. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 338, n.6 (2016) (“named plaintiffs who represent a class ‘must ... show that they personally have been injured’”) (citation omitted); *see also Easter v. Am. W. Fin.*, 381 F.3d 948, 962 (9th Cir. 2004) (“The district court correctly addressed the issue of standing

before ... the issue of class certification.”). Plaintiffs must show “(i) that [they] suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant, and (iii) that the injury would likely be redressed by judicial relief.” TransUnion LLC v. Ramirez, 594 U.S. 413, 423 (2021) (citation omitted).

Where, as here, the Court is faced with an intangible harm caused by a statutory violation, it must determine whether the statutory provision at issue is a “bare procedural protection”—in which case Plaintiffs must link a violation to a concrete harm to establish standing—or is instead “a substantive right,” the violation of which is a de facto injury that is itself enough to show harm. Campbell v. Facebook, Inc., 951 F.3d 1106, 1117 (9th Cir. 2020) (first quoting Spokeo, 578 U.S. at 341–42, and then citing Eichenberger v. ESPN, Inc., 876 F.3d 979, 983–84 (9th Cir. 2017)).

B. Discussion

In Campbell, the Ninth Circuit held that the CIPA provision at issue here—California Penal Code section 631(a)—implicates a “substantive right,” the violation of which is enough to cause concrete and particularized harms and give rise to Article III standing. Id. at 1118–19. The panel reasoned that section 631(a) was closely related to the common law tort of unreasonable intrusion upon seclusion, which traditionally extended to provide a remedy for wiretapping and the opening of private mail. Id. at 1112. It also explained that section 631(a) reflected the “legislature’s judgement about the importance of the privacy interests violated when communications are intercepted” and concern about “the use of new technology to ‘eavesdrop[] upon private communications.’” See id. at 1118 (citation omitted). Plaintiffs’ allegations are substantially the same as those in Campbell.

Furthermore, because Campbell held that the interception of communications without consent is itself an Article III injury, id. at 1118–19, Plaintiffs do not need to show that they had input their own private information (as opposed to someone else’s) in the form or that the data Defendants allegedly collected was put to any improper use. Of course, if such allegations are substantiated, that might subject Defendants to additional

liability. See In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 599, 601 (9th Cir. 2020) (listing other potentially viable statutory and common-law claims). But for standing purposes, all that Plaintiffs must allege is that Defendants “collect[ed] the contents of users’ individual private messages ... without [Plaintiffs’] consent.” Campbell, 951 F.3d at 1119. “[H]ow the collected data was later used is irrelevant.” Id. Plaintiffs’ allegations are thus sufficient to establish their standing under Article III.

III. CLASS CERTIFICATION

A. Legal Standard

Rule 23, which governs class actions, requires that plaintiffs meet the requirements of Rule 23(a), as well as one of three possible requirements under Rule 23(b). Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 615 (1997). Rule 23(a) requires (1) that “the class is so numerous that joinder of all members is impracticable,” (2) that “there are questions of law or fact common to the class,” (3) that “the claims or defenses of the representative parties are typical of the claims or defenses of the class,” and (4) that “the representative parties will fairly and adequately protect the interests of the class.” Plaintiffs must establish these elements by a preponderance of the evidence. Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC, 31 F.4th 651, 664–65 (9th Cir. 2022) (en banc).

Plaintiffs seek certification under Rule 23(b)(3), which requires additionally that “the questions of law or fact common to class members predominate over any questions affecting only individual members” and that “a class action [be] superior to other available methods for fairly and efficiently adjudicating the controversy.” To establish that certification is appropriate, plaintiffs may use any admissible evidence. Id. at 665. The Court may evaluate the merits of Plaintiffs’ case, but only to the extent “that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied.” Amgen, Inc. v. Conn. Ret. Plans. & Tr. Funds, 568 U.S. 455, 466 (2013).

B. Discussion

Defendants do not appear to contest that Plaintiffs satisfy the Rule 23(a) requirements—numerosity, typicality, typicality, and adequacy—or the Rule 23(b)(3)

1 requirement of superiority.³ Rather, Defendants argue that common questions do not
 2 predominate over three allegedly individualized inquiries: (1) whether class members
 3 impliedly consented to ActiveProspect’s real-time interception of their information,
 4 (2) whether purported class members are in fact eligible class members, and (3) whether
 5 the alleged interception occurred in California. Opp. at 1–2.

6 “The predominance inquiry ‘asks whether the common, aggregation-enabling,
 7 issues in the case are more prevalent or important than the non-common, aggregation-
 8 defeating, individual issues.’” Tyson Foods, Inc. v. Bouaphakeo, 577 U.S. 442, 543
 9 (2016) (citation omitted). A common question “must be of such a nature that it is capable
 10 of class wide resolution—which means that the determination of its truth or falsity will
 11 resolve an issue that is central to the validity of each one of the claims in one stroke.”
 12 Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350 (2011). Individual questions,
 13 meanwhile, require “members of a proposed class ... to present evidence that varies from
 14 member to member.” Olean Wholesale Grocery, 31 F.4th at 663 (citation omitted).

15 “Considering whether ‘questions of law or fact common to class members
 16 predominate’ begins, of course, with the elements of the underlying cause of action.”
 17 Erica P. John Fund, Inc. v. Halliburton Co., 563 U.S. 804, 809 (2011) (quoting Fed. R.
 18 Civ. P. 23(b)(3)). Under CIPA, Plaintiffs must show that ActiveProspect (1) willfully
 19 (2) and without Plaintiffs’ consent (3) read or attempted to read or learn the contents of
 20 their communications (4) while the communications were being sent from, received in, or
 21 in transit or passing over any wire, line or cable in California. Id.

22 Plaintiffs identify, and Defendants do not appear to dispute, the existence of several
 23 common questions, such as:

- 24 • Whether ActiveProspect acted willfully. Mot. to Certify Class (dkt. 66) at 9.
- 25 • Whether the information that users provided to obtain a life insurance quote
- 26 was “content” as covered by CIPA. Id.; see also Katz-Lacabe v. Oracle Am.,

27
 28 ³ Neither do Defendants contest the portion of Plaintiffs’ motion where Plaintiffs seek to
 appoint themselves as class representatives and Girard Sharp LLP as class counsel.

Inc., 668 F. Supp. 3d 928, 944 (N.D. Cal. 2023) (“content” under CIPA “refers to the intended message conveyed by the communication,” not “information about the characteristics of the message” (citation omitted)).

- Whether the information was intercepted while it was “in transit.” Mot. to Certify Class at 10.
- Whether Prudential and Assurance aided ActiveProspect’s alleged violation. Id. at 12.
- Classwide damages. See Cal. Penal Code § 637.2(a)(1) (providing statutory damages of \$5,000 per violation).

Defendants dispute, however, that common proof can be used to show:

- Whether class members consented to ActiveProspect’s alleged interception of their communications. Opp. at 1.
- Whether a class member filled out Prudential’s form. Id. at 2. (Defendants say this is relevant to show that the class member was injured. Id. at 12.)
- Whether ActiveProspect intercepted class members’ communications while they were “in transit or passing over any wire, line, or cable, ... sent from, or received at any place within [California].” Id. at 2; see Cal. Penal Code § 631(a).

1. Implied Consent

Defendants contend that individualized questions regarding each class member’s consent defeats predominance.⁴ Opp. at 6.

“[C]onsent ‘can be express or implied.’” Calhoun v. Google, LLC, 113 F.4th 1141, 1147 (9th Cir. 2024) (cleaned up) (citations omitted). Defendants do not dispute that,

⁴ At the outset, the parties dispute who has the burden of proving or disproving consent. Compare Opp. at 6, with Reply (dkt. 90) at 4 n.1. Courts in this District hold that the defendant must prove consent. E.g., Brown v. Google LLC, 685 F. Supp. 3d 909, 926, n.13 (N.D. Cal. 2023). Regardless, who bears the burden of proof is a common question and is irrelevant to class certification. See Adams v. Ins. Co. of N. Am., 436 F. Supp. 2d 356, 360–61 (S.D. W. Va. 2006) (recognizing that “the applicable burden of proof” is a common question).

during the class period, they did not obtain prior express consent from users for the challenged data collection. See Renz Dep. Tr. (dkt. 64-8) at 157:4-22. Rather, they focus on the question of implied consent. See Opp. 6–7. To establish implied consent, “the circumstances, considered as a whole, [must] demonstrate that a reasonable person [would have] understood that [the] action[s] would be carried out” and that they proceeded to expose themselves to the actions anyways. Calhoun, 113 F.4th at 1147 (citation omitted). It is important to recognize, however, that “what a ‘reasonable user’ of a service would understand they were consenting to” is “not what a technical expert would.” Id. at 1149. “Consent is only effective if the person alleging harm consented ‘to the particular conduct, or substantially the same conduct.’” Id. at 1147 (cleaned up) (citation omitted).

Defendants contend that four sources of information would have given notice of the challenged conduct: (1) Assurance’s privacy policy; (2) Prudential’s privacy policies; (3) a consumer survey conducted by their expert, Dr. Mathiowitz; and (4) third-party material, including news articles about session replay software and legal advertisements. Opp. at 8–11. And they assert that the inquiry into whether each class member was exposed to any of these sources is an individualized one that undermines predominance. Id.

Assurance’s Privacy Policy. Defendants first argue that class members who had previously used a “substantially similar” form on Assurance’s website and assented to Assurance’s privacy policy were likely aware of ActiveProspect’s interception of their data on Prudential’s form. Id. at 8–9. In support of their argument, Defendants point to this Court’s orders regarding a motion to dismiss in Javier v. Assurance IQ, LLC. See 649 F. Supp. 3d 891, 896–97 (N.D. Cal. 2023) (granting motion to dismiss); No. 20-CV-02860-CRB, 2023 WL 3933070 (N.D. Cal. June 9, 2023) (granting motion to dismiss amended complaint). Those orders do not support Defendants’ position here.

In Javier, the plaintiff sued Assurance and ActiveProspect (two of the same defendants as here) under section 631(a) for similar conduct as Plaintiffs allege here. 649 F. Supp. 3d at 894–95. The plaintiff, however, filed his lawsuit fifteen months after he visited Assurance’s website—three months too late under CIPA’s statute of limitations.

Id. at 901. He tried to invoke the delayed discovery doctrine, which would have required him to allege that he could not have known about the alleged CIPA violation until a later date within the limitations period. Id. But this Court rejected his argument, explaining that Assurance’s privacy policy (which the plaintiff had accepted the terms of during his visit to Assurance’s website) put him on “inquiry notice” that his information had been collected, even if he did not know the details of the collection (including exactly who collected his data) at that time. Id. at 902.

Defendants fail to explain why the standard for inquiry notice for statute-of-limitations purposes should be applied to determine if Plaintiffs actually consented to the interception of their communications. To the contrary, Javier clearly states that the two standards are different. This Court expressly rejected the defendants’ contention that the plaintiff had impliedly consented to ActiveProspect’s collection of his information using TrustedForm—essentially the same contention that the same defendants make in this case. 649 F. Supp. 3d at 896–97. This Court explained that there was no evidence that Javier had notice of ActiveProspect’s collection of his data until he agreed to Assurance’s privacy policy. Id. at 896. And this Court declined to find implied consent on the theory (which Defendants seem to advance a version of here) that the plaintiff’s mere use of a website to obtain an insurance quote is enough to show that he impliedly consented to the monitoring of his information. Id. at 897.

Defendants’ argument that any potential class members in this case who filled out a form on Assurance’s website impliedly consented to monitoring by ActiveProspect given their prior awareness of Assurance’s privacy policy is too strained to defeat predominance. See Rodriguez v. Google LLC, No. 20-CV-04688-RS, 2024 WL 38302, at * 9 (N.D. Cal. Jan. 3, 2024) (the “relevant question” as to consent inquiry under CIPA concerns website operator’s disclosures about its data collection practices, not third-party disclosures about operator’s practices); see also Calhoun, 113 F.4th at 1147 (“[C]ircumstances, considered as a whole,” must “demonstrate that a reasonable person would have understood that an action would be carried out so that their acquiescence demonstrates knowing

1 authorization.” (citation omitted)).

2 **Prudential’s Privacy Policies.** Prudential argues that its privacy policies, which
3 were accessible through a hyperlink in the footer of every page of its website, provided
4 notice of the challenged data practice, thus raising an individualized question as to which
5 class members read the disclosures before filling out the form. Opp. at 8; Prudential
6 Privacy Notice (dkt. 66-16), Prudential CCPA Disclosure (dkt. 66-17). Plaintiffs identify a
7 threshold problem with that argument—they challenge whether the privacy policies
8 provided notice of the challenged practice at all. Mot. to Certify Class at 5. They assert
9 that that is a common question, as Prudential’s privacy policy remained the same during
10 the class period. *Id.* (citing Renz Dep. Tr. at 261:3–20).

11 The Court agrees with Plaintiffs that Prudential’s Privacy Notice and its CCPA
12 Disclosure likely would not put a reasonable person on explicit notice of ActiveProspect’s
13 real-time interception of their every interaction, keystroke by keystroke, with Prudential’s
14 form. Prudential’s Privacy Notice describes various types of personal information that
15 Prudential collects when users fill out its form, including “medical information for
16 insurance applications” and “information gathered from your internet or network activity.”
17 Prudential Privacy Notice at 2. But a reasonable person would probably not expect
18 collected information to include their every keystroke—including information that a user
19 enters and then deletes prior submitting the form, which neither the website operator nor
20 any third party would ever see but for real-time tracking.⁵ See Yockey v. Salesforce, Inc.,

21
22 ⁵ Indeed, news articles that Defendants themselves cite indicate that people generally do
23 not expect the extent of data collection that session replay technology enables. *E.g.*,
24 Louise Marsakis, Over 400 of the World’s Most Popular Websites Record Your Every
25 Keystroke, Princeton Researchers Find, Vice (Nov. 20, 2017), [https://perma.cc/BFP6-](https://perma.cc/BFP6-NRQZ)
26 [NRQZ](https://perma.cc/BFP6-NRQZ) (noting that while “[m]ost people who’ve spent time on the internet have some
27 [understanding that many websites log their visits and keep record of what pages they’ve](https://perma.cc/BFP6-NRQZ)
28 [looked at,” session replay technology enables “online tracking \[that\] is far more invasive](https://perma.cc/BFP6-NRQZ)
[than most users understand.”](https://perma.cc/BFP6-NRQZ) (emphasis added)); Steven Englehardt, No Boundaries:
Exfiltration of Personal Data by Session-Replay Scripts, Freedom to Tinker (Nov. 15,
2017), <https://perma.cc/5ZTB-7M2E> (“You may know that most websites have third-party
analytics scripts that record which pages you visit and the searches you make. ... However
the extent of data collected ... far exceeds user expectations; text typed into forms is
collected before the user submits the form, and precise mouse movements are saved, all
without any indication to the user.”); Sidney Fussell, The Analysts Recording Your Screen

688 F.Supp.3d 962, 977 (N.D. Cal. 2023) (privacy policy disclosing that the defendant could “share [customers’] personal information ... with third parties” did not disclose third party’s “word-for-word” recording of all chat messages sent to the defendant’s customer service agent “while [customers] type[d] them”).

Prudential’s Privacy Notice states that it “may share your personal information ... among Prudential companies and with other non-Prudential companies who perform services for us or on our behalf, for our everyday business purposes, such as providing services to you, [and] administering your account or policy.” Prudential Privacy Notice at 2 (emphasis added). And Prudential’s CCPA Disclosure states that it “collect[s], use[s], and disclose[s]” personal information relating to California residents. Prudential CCPA Disclosure at 3 (emphasis added). Neither of these disclosures is likely to lead a reasonable user to expect that a third party itself collects their personal information in real time, however; they instead suggest that Prudential shares that information so third parties can “perform services for [Prudential] or on [Prudential’s] behalf.” Prudential Privacy Notice at 2; see also Prudential CCPA Disclosure at 5 (describing categories of user personal information disclosed to third-party service providers).

In any case, Plaintiffs are correct that the issue of how a reasonable user would understand Prudential’s privacy policies is a common one that can be resolved with class-wide proof. See Amgen, 568 U.S. at 466; Calhoun, 113 F.4th at 1148; Frasco v. Flo Health, Inc., No. 21-CV-00757-JD, 2024 WL 4280933, *2 (N.D. Cal. Sept. 23, 2024) (jury can resolve factual disputes as to “scope of plaintiffs’ consent to sharing data”). If a factfinder determines that a reasonable user would understand Prudential’s privacy policies in such a way that those policies confer consent, the Court can then evaluate whether the effort required to ascertain which class members read the privacy policies would defeat predominance. See Officers for Just. v. Civil Serv. Comm’n, 688 F.2d 615, 633 (9th Cir.

Say It’s for Your Own Good, The Atlantic (Feb. 12, 2019), <https://perma.cc/6785-LLZ9> (“[I]nherent to the session replay is the idea that customers are most valuable when they don’t know they’re being watched.”).

1 1982) (“[A] district court’s order respecting class status is not final or irrevocable, but
2 rather, it is inherently tentative.” (citations omitted)).

3 **Dr. Mathiowitz’s Survey.** Defendants next argue that Dr. Mathiowitz’s survey
4 raises individualized questions about whether “class members knew about the alleged
5 interceptions and nevertheless used the [form].” Opp. at 11. The survey results suggest
6 that there is variation among consumers’ expectations about whether a third-party software
7 collects information on a website that provides life insurance quotes. Mathiowitz Rpt.
8 (dkt. 81-8) at 7. But these results say nothing about whether class members were likely to
9 have explicit notice about the specific data collection at issue here, see Calhoun, 113 F.4th
10 at 1147, or whether they knew that it was likely to occur, see United States v. Staves, 383
11 F.3d 977, 981 (9th Cir. 2004) (in the context of cellphone monitoring, “the circumstances
12 must indicate that a party to the communication knew that interception was likely and
13 agreed to the monitoring” (citation omitted)); In re Google Inc., No. 13-MD-02430-LHK,
14 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013) (“That [a] person communicating
15 knows that [an] interceptor has the capacity to monitor the communication is insufficient
16 to establish implied consent.”). Accordingly, Dr. Mathiowitz’s survey is not determinative
17 for purposes of this motion.⁶

18 **Third-Party Materials.** Defendants next argue that the issue of consent defeats
19 predominance because third-party materials, such as news articles and advertisements,
20 could have informed class members about the challenged data interceptions at issue here
21 before they filled out Prudential’s form. Opp. at 9. They specifically identify the
22 following materials:

- 23 • News articles about how session replay technology works generally and its
24 use on various “popular” and “major” consumer-facing websites such as
25 Facebook, Papa John’s, Bank of America, and Walgreens. See Opp. Ex. 20
26 (dkt. 81-21) at 6, 19–22, 41, 51–52 (collecting news articles). None of these

27
28 ⁶ The pending motion to strike Dr. Mathiowitz’s report (dkt 89) is therefore moot. This
does not preclude Plaintiffs from raising future Daubert challenges as to Dr. Mathiowitz.

articles discuss the technology’s use on consumer-facing insurance websites, nor do they mention Prudential, Assurance, or ActiveProspect.

- A law firm advertisement stating: “If you used Prudential’s website to get a life insurance quote, you may be entitled to compensation due to a possible privacy violation.” Don Bivens PLLC Advertisement (dkt. 81-20).
- Coverage and analysis of the Javier case on legal blogs and news websites. See Eric Goldman, Consent Via “Clickwrap” Defeats Privacy Claims—Javier v. Assurance, Tech. & Mktg. L. Blog (Mar. 14, 2021), <https://perma.cc/A57V-YS2Q>.
- A November 30, 2022 article on a website called “Life Annuity Specialist” about the instant case. See Opp. Ex. 11 (dkt. 81-12). The article states that “[Prudential’s] use of third-party software to record prospective buyers’ website activity violates California privacy laws.” Id.

To be sure, the “factfinder, in determining whether class members impliedly consented to the alleged conduct[,] would have to determine the sources of information to which each was exposed.” Brown v. Google, LLC, No. 20-CV-3664-YGR, 2022 WL 17961497, at *19 (N.D. Cal. Dec. 12, 2022). But once again there is a threshold common question whether any of the sources provided notice of the challenged conduct in the first place. Here, only one of Defendants’ sources—the Life Annuity Specialist article—could be capable of providing the kind of notice required to establish consent, and that article was published just a few weeks before the end of the class period. The news articles and law firm advertisements, in contrast, are too general to give explicit notice to the particular conduct at issue here, either because they discuss session replay technology in different contexts or because they do not disclose Prudential’s relationship with Assurance and ActiveProspect. See Calhoun, 113 F.4th at 1147; accord Campbell v. Facebook, Inc., 315 F.R.D. 250, 266 (N.D. Cal. 2016) (news source that did not disclose specific conduct at issue incapable of giving notice).

Therefore, none of these sources create an individualized implied-consent inquiry

1 that would predominate over common questions or threaten to make adjudication
 2 unmanageable. To the extent that the Life Annuity Specialist article provides sufficient
 3 notice to establish implied consent, the Court can later refine the class period to exclude
 4 any class members that might have seen the article. See Olean Wholesale Grocery, 31
 5 F.4th at 670, n.14 (“[T]he problem of a potentially ‘over-inclusive’ class ‘can and often
 6 should be solved by refining the class definition rather than by flatly denying class
 7 certification on that basis.’” (citation omitted)).

8 **2. Identification of Class Members**

9 Defendants next argue that Plaintiffs’ proposed method for identifying injured class
 10 members—by reference to Assurance’s database of inputs in the Prudential form—is
 11 flawed because at least some class members filled out the Prudential form on behalf of
 12 others. Opp. at 1. So, Defendants assert, the database can only be used to identify
 13 individuals on whose behalf class members filled out the form, which may or may not be
 14 the same person who actually filled out the form. Id. at 2. Defendants characterize this as
 15 an individualized inquiry into class members’ standing under CIPA. Id. Plaintiffs counter
 16 that Defendants mischaracterize the standing inquiry and that “identifying class members
 17 is not grounds for denying class certification.” Reply at 12–14.

18 As part of the predominance inquiry, “a court must consider whether the possible
 19 presence of uninjured class members means that [a] class definition is fatally overbroad.”
 20 Olean Wholesale Grocery, 31 F.4th at 669, n.14. This would be the case if, for instance,
 21 the class includes “a great number of members who for some reason could not have been
 22 harmed by the defendant’s allegedly unlawful conduct.” Id. (citation omitted) (emphasis
 23 added); see also Moore v. Apple, 309 F.R.D. 532, 534 (N.D. Cal. 2015) (denying
 24 certification of a class that included individuals who, based on the class definition, “could
 25 not have been injured by Defendant’s allegedly wrongful conduct”) (emphasis in original).
 26 Defendants do not actually argue that the proposed class is overbroad, though; they seem
 27 to instead contend that “there is [no] administratively feasible way to determine who is in
 28 the class.” See Briseno v. ConAgra Foods, Inc., 844 F.3d 1121, 1125 (9th Cir. 2017). Yet

there is no feasibility requirement in the Ninth Circuit. Id. (declining to require plaintiffs to “propose [a] way to identify class members and [] prove that an administratively feasible method exists [to do so]” at the class certification stage).

Moreover, Plaintiffs contend that they can identify class members using Assurance’s database. They point out that one of the Plaintiffs filled out a form for a life insurance quote on behalf of her herself (on Prudential’s website) and her father (on Assurance’s website) and provided her own e-mail address and phone number in both forms. Reply at 13 (citing *Jornaya Guardian TCPA Rpt.* (dkt. 81-17), and *Hyman Dep. Tr.* (dkt. 91-6) at 92:10–15). Defendants were able to cross-reference her contact information to identify which form she submitted on behalf of her father. Id. In addition to this cross-reference method, the Court can require class members to present an affidavit that a submission was theirs. See Kellman v. Spokeo, Inc., No. 21-CV-08976-WHO, 2024 WL 2788418 (N.D. Cal. May 29, 2024) (whether class members’ names and addresses matched ones in online profile could be established via affidavit (citing *Briseno*, 844 F.3d at 1132)).

Plaintiffs have shown that Defendants’ records are “capable of showing” which individuals filled out the Prudential form and had their communication intercepted; that is “all that [is] necessary at the certification stage.” See Olean Wholesale Grocery, 31 F.4th at 680–81 (emphasis in original).

3. Location of Interception

Next, Defendants argue that Assurance’s database, which collects the IP addresses of users who submitted the Prudential form, is not enough to show that communications were intercepted in California because some class members could have used a virtual private network (VPN) to obscure their IP address.⁷ Opp. at 13 (citing *Polish Decl.* (dkt. 81-24) ¶¶ 9, 11–17). As support, Defendants rely on Dr. Mathiowitz’s consumer survey regarding the prevalence of VPN use as well as Dr. Polish’s expert opinion

⁷ Dr. Polish explains how VPNs work: “[W]hen an Internet user connects to the Internet using a VPN, the user’s network traffic appears as though it is emerging from the VPN generated location instead of the user’s actual physical location.” *Polish Decl.* ¶ 14.

1 discussing how VPNs work. See Mathiowetz Rpt. ¶¶ 46–48; Polish Decl.

2 As a threshold matter, Defendants frame the location inquiry too narrowly. CIPA is
3 not just concerned with whether communications were sent from a place in California; it
4 also covers communications intercepted while “in transit or passing over any wire, line, or
5 cable” in California or “received at any place” in California. See Cal. Penal Code
6 § 631(a). But in any case, neither Dr. Mathiowetz’s survey or Dr. Polish’s report leads the
7 Court to conclude that the question whether interception occurred in California is more
8 prevalent or important than the other, common issues in this case. See Tyson Foods, 577
9 U.S. at 543. Dr. Mathiowetz’s survey results indicate that only 17.7% of those surveyed
10 (consumers living in California in 2022 who had shopped online for a life insurance quote
11 since January 2022) “always” or “sometimes” used a VPN when using the Internet for
12 personal use. Mathiowetz Rpt., tbl. 1, ¶¶ 30, 48. And Dr. Polish opines simply that “[a]n
13 Internet user’s IP address is not necessarily a reliable indicator of that individual’s
14 geographic location.” Polish Decl. ¶¶ 9, 13. Neither expert’s testimony actually quantifies
15 the number of potential class members who use a VPN to access life insurance websites or
16 whose VPN would locate them in a different state.

17 Plaintiffs additionally contend that Assurance’s database could easily be used to
18 identify any potential class members who used a VPN by cross-referencing a class
19 member’s ZIP code with their IP address. Reply at 14. Where the data points indicate
20 different locations, class members may be required to attest via affidavit to their location at
21 the time they filled out the form. See Zaklit v. Nationstar Mortg. LLC,
22 No. 515CV2190CASKKX, 2017 WL 3174901, at *9 (C.D. Cal. July 24, 2017) (for
23 purposes of CIPA, “it is ‘more likely than not that a person with a California area code
24 [was] located in California’”). Because this method is capable of identifying class members
25 who filled out the form while in California, the issue of location does not defeat
26 predominance.

IV. CONCLUSION

For the foregoing reasons, the Court **CERTIFIES** the following class in this action:

All natural persons who, while in California, visited Prudential.com, provided personal information on Prudential's form to receive a quote for life insurance, and for whom a TrustedForm Certificate URL associated with that website visit was generated from November 23, 2021 to December 13, 2022.

The Court also **APPOINTS** Girard Sharp LLP as class counsel and Valerie Torres and Rhonda Hyman as class representatives.

IT IS SO ORDERED.

Dated: November 26, 2024



CHARLES R. BREYER
United States District Judge